Homeland and Industrial Control Security

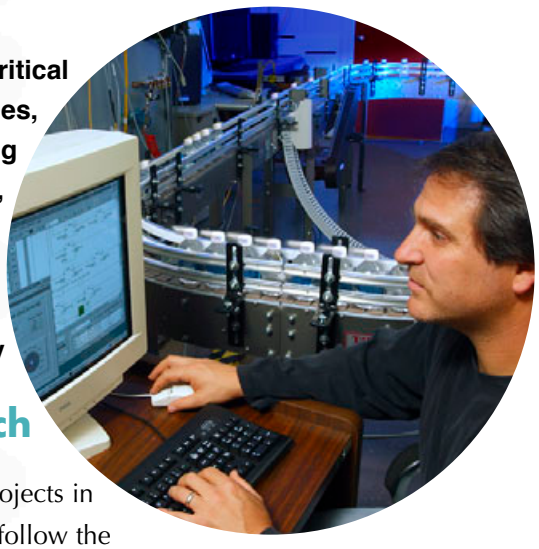
Program Manager:	Al Wavering
Phone:	301 975 3461
Email:	albert.wavering@nist.gov
Program Funding:	$3.5 M
FTEs:	8.8

Program Goal

Develop and apply MEL capabilities, tools, and methods to enhance: Preparation for, prevention of, defense against, and response to threats and aggressions against the domestic population and infrastructure of the United States; and Effectiveness of domestic emergency response and law.

Problem

The Department of Homeland Security (DHS) and federal, state, and local emergency response agencies and personnel need an integrated infrastructure of performance metrics, test methods and standards to 1) enable specification, evaluation, and integration of homeland security and public safety equipment and systems, and 2) encourage investment in homeland security science and technology efforts. The lack of consensus in national requirements and standards slows development and leads to confusion among both suppliers and users of homeland security technologies. In coordination with related efforts internal and external to NIST, the MEL Homeland and Industrial Control Security (H&ICS) Program helps build this standards infrastructure, primarily in areas that cut across multiple vulnerability, threat, and response mode categories.



Securing critical industries, including water, electrical power, and chemical is a top priority

Approach

In general, projects in this program follow the approach used for all DHS standards development and implementation projects. For each component or system under consideration, guidelines will be developed as a collaborative effort among tool developers, users/subject matter experts, and standards experts. Requirements and guidelines will be defined using information related to the capabilities – and the limitations - of the components, and on the conditions in which the component and system are expected to operate. The guidelines will be the foundation for constructing performance measures and testing and evaluation protocols that will provide a reproducible method for assessing and comparing the effectiveness of each system component and of the systems supporting homeland security. Performance measures will encompass: basic functionality, adequacy and appropriateness for the task, interoperability, efficiency, and sustainability.

Typical Customers and Collaborators

Department of Homeland Security Science & Technology and Emergency Preparedness and Response Directorates, National Institute of Justice, ISA: the Society for Instrumentation, Systems, and Automation, Institute of Electrical and Electronics Engineers (IEEE), Critical Infrastructure owner-operators and suppliers, and the Department of Defense.

For more information see page 44

homeland security

Homeland and Industrial Control Security

Program Goal

Develop and apply MEL capabilities, tools, and methods to enhance:

- Preparation for, prevention of, defense against, and response to threats and aggressions against the domestic population and infrastructure of the United States
- Effectiveness of domestic emergency response and law enforcement

Program Manager:
Al Wavering

Total FTEs:
8.8

Annual Program Funds
$3.5 M

Customer Need and Intended Impact

The Department of Homeland Security (DHS) and federal, state, and local emergency response agencies and personnel need an integrated infrastructure of performance metrics, test methods and standards to 1) enable specification, evaluation, and integration of homeland security and public safety equipment and systems, and 2) encourage investment in homeland security science and technology efforts.[1] The lack of consensus national requirements and standards slows development and leads to confusion in the private sector (e.g., equipment manufacturers, software developers, and shippers) and the government sector (e.g., Federal Emergency Management Agency (FEMA), and state and local emergency planners). In coordination with related efforts internal and external to NIST, the MEL Homeland and Industrial Control Security (H&ICS) Program helps build this standards infrastructure, primarily in areas that cut across multiple vulnerability, threat, and response mode categories.

In addition to federal agency needs, U.S. manufacturers have measurement and standards needs related to securing their own operations and to ensuring that their entire network of supporting services and distributed means of production are able to continue unimpeded. Uninterrupted national and international transportation of parts, subassemblies, and finished goods, continuous flow of power, oil and gas, and chemicals, and robust, secure communication of supply chain information are of paramount importance to manufacturers.[2]

[1] National Strategy for Homeland Security, Office of Homeland Security, July 2002, http://www.dhs.gov/dhspublic/display?theme=85&content=285.

[2] Manufacturing in America: A Comprehensive Strategy to Address the Challenges to US Manufacturers, US Department of Commerce, Washington, DC, January 2004, available at http://www.manufacturing.gov/.

The ultimate outcome of this program is for federal, state, emergency response, and law enforcement agencies to obtain the best value for their investment in homeland security technologies, to save lives and property through broader deployment of the technologies, and to enable technology developers to accelerate development of advanced capabilities. In addition, many H&ICS projects may result in dual-use benefits. For example, improved knowledge of shipping container contents and location improves security and also improves production scheduling. The H&ICS program responsively addresses new and changing needs of our customers that have arisen post September 11, 2001.

Technical Approach & Program Objectives

In general, projects in this program will follow the same approach used for DHS standards development and implementation projects, illustrated in Figure 1 below. For each component or system under consideration, guidelines will be developed as a collaborative effort among tool developers, users/subject matter experts, and standards experts. Requirements and guidelines will be defined using information related to the capabilities – and the limitations - of the components, and on the conditions in which the component and system are expected to operate. The guidelines will be the foundation for constructing performance measures, and testing and

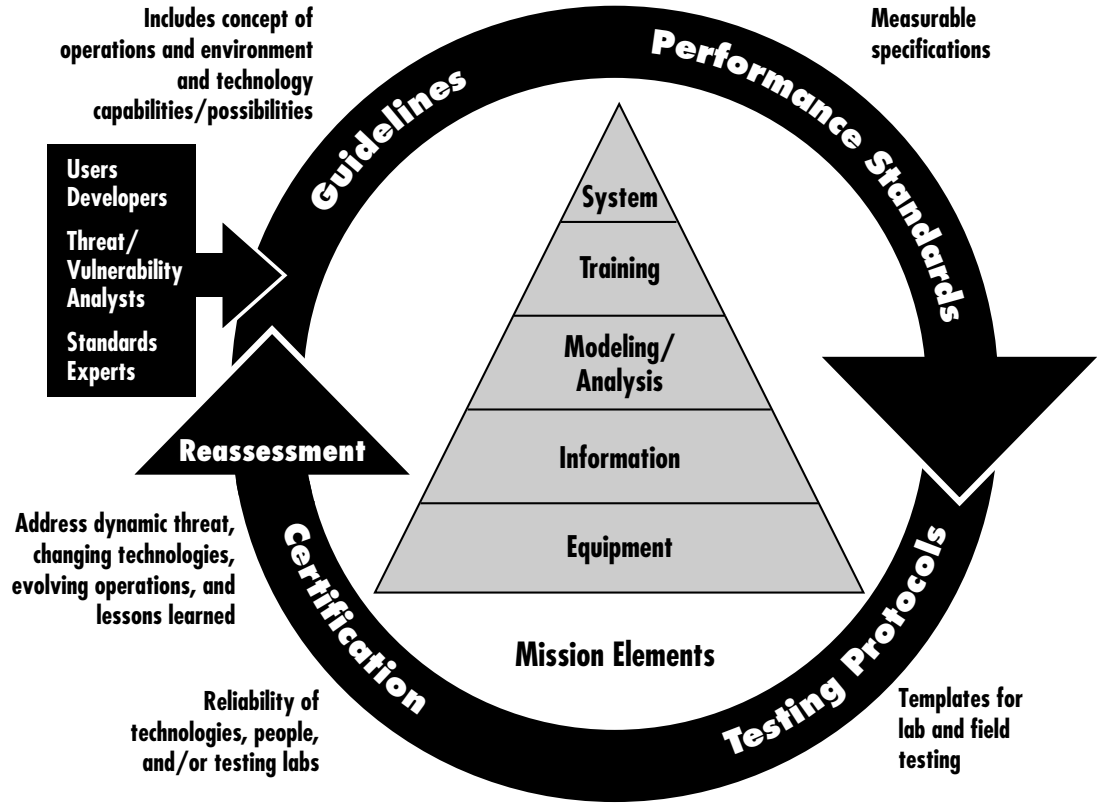


Figure 1. Process for managing DHS standards for all elements of the mission.[3]

[3] Source: Bert Coursey, Standards Program Manager, DHS Science and Technology Directorate.

evaluation protocols that will provide a reproducible method for assessing and comparing the effectiveness of each system component and of the systems supporting homeland security. Performance measures will encompass basic functionality, adequacy and appropriateness for the task, interoperability, efficiency, and sustainability.

One of the key parts of the national measurements and standards infrastructure for homeland security hardware, software and processes is the development of consensus performance standards. Standards Development Organizations (SDOs) with relevant interest and expertise are identified for each technical area to be addressed. This program leverages this existing expertise by establishing a working relationship between these SDOs and other federal agencies to develop consensus requirements and performance standards for system products and processes.

Objectives

Objective #1:
Define and apply performance metrics and standards for homeland security robots,

Objective #2:
Define and apply information security requirements, standards, and test methods for industrial control systems,

Objective #3:
Develop standards for integrating simulation systems and databases for advanced planning, training, and event decision support,

Objective #4:
Lay the groundwork for development of a standards-based framework for homeland security smart sensor networks,

Objective #5:
Demonstrate the benefits of Bullet and Casing Reference Materials for verification of equipment in law enforcement laboratories performing ballistics signature comparisons,

Objective #6:
Evaluate the feasibility of extending the concept of "firearms identification" to develop a national ballistics database for all firearms sold in the U.S.,

Objective #7:
Provide an in-depth understanding of bullet and armor materials leading to predictive models and computer simulations of bullet/armor interactions,

Objective #8:
Complete revisions of standards and guides for emergency vehicle sirens.

Major Accomplishments

- Conducted three urban search and rescue (US&R) Robot Competitions to help accelerate the development of US&R robot technologies: RoboCup2004 U.S. Open Rescue Robot Competition (New Orleans, LA), RoboCup2004 Rescue Robot Competition (Lisbon, Portugal), AAAI2004 Rescue Robot Competition (San Jose, CA)
- Launched DHS-funded multi-year program to develop comprehensive standards and performance metrics for US&R robots
- Released for public comment draft System Protection Profile for Industrial Control Systems, which outlines security requirements to help utilities and other critical infrastructure industries secure their industrial control systems
- Tested compatibility of antivirus software with control system operator interfaces in the Industrial Control System Security Testbed. The test results help industry understand how to select the most appropriate antivirus software configuration settings in an operational control system environment
- Developed Industrial Ethernet performance tests and helped conduct industry-wide testing events, improving the robustness and interoperability of Industrial Ethernet implementations
- Held Modeling and Simulation for Emergency Response Workshop at NIST March 2-3, 2004, resulting in a draft Roadmap for Integrated Modeling & Simulation for Emergency Response

FY2005 Projects

Homeland Security Robot Performance Metrics and Standards (Objective #1)

DHS and other agencies are actively exploring the application of ground, air, and underwater robots to a number of homeland security applications, and need an infrastructure of standard requirements and performance metrics for robot systems and components to help them obtain the greatest benefit from this technology. The requirements will provide concrete performance targets and drive robot development. Performance metrics will give agencies a means to evaluate what they are getting for their money. Without standards and metrics, equipment purchasers have only supplier claims and demonstrations to rely upon. Furthermore, standards are needed to enable robotic technology to be developed on a modular component basis, which enables best-of-breed systems to be assembled. The project has three current thrusts aimed at addressing these needs: 1) developing reference test arenas and conducting competitions for urban search and rescue (US&R) robots (NIST-funded), 2) developing performance metrics and standards for US&R robots (DHS-funded), and 3) defining performance metrics for bomb disposal robots (National Institute of Justice (NIJ)-funded).

Industrial Control System Security (Objective #2)

Foreign adversaries have singled out critical infrastructures as strategic targets for physical and cyber attack.[4] While many security experts agree that physical attacks are the most immediate threat to critical infrastructures, they recognize the need to secure industrial control systems from cyber attack as well. [5, 6, 7] Two primary categories of standards are needed for industrial control system security. Standard security requirements are needed so owner- operators know what to specify, and so suppliers know what to build. Standard performance test methods are needed to evaluate the impact of security technologies on real-time control system behavior and to measure the performance of control system network components. We are working with other federal agencies and industry representatives in this project to address both of these needs.
A broad cross section of industrial control system users and suppliers participate in this effort through the NIST-led Process Control Security Requirements Forum (PCSRF).

Modeling and Simulation for Emergency Response (Objective #3)

While there are numerous stand-alone modeling and simulation tools for specific homeland security-related domains, these tools need to be brought together for studying the impact of disaster events as a whole. Currently, there are no standards that define the data interfaces, database structures, or software architectures for relevant emergency response simulation and visualization applications. Interoperability standards for simulation and visualization tools for emergency response could significantly improve the Nation's capabilities in this area. An integrated set of simulations could be used for developing well-coordinated response plans. They could be used for providing a complete scenario for training where the results of response actions can be evaluated immediately allowing rapid learning for the trainees. The tools could also be used for rapid evaluation of alternate response plans to a major incident and assist in a prudent selection of the plan leading to minimization of impact from the incident. The needs and a proposed approach to addressing them have been well documented as a result of two workshops on Modeling and Simulation for Emergency Response sponsored by NIST in 2003 and 2004.[8,9] This project builds on the results of these workshops toward establishing a standards framework for emergency response simulations.

[4] Unclassified CIA threat briefing at NIST, July 9, 2004.

[5] Challenges and Efforts to Secure Control Systems, GAO 04-354, March 2004

[6] Manufacturing in America: A Comprehensive Strategy to Address the Challenges to US Manufacturers

[7] Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

[8] Modeling and Simulation for Emergency Response: Workshop Report, Standards and Tools, Sanjay Jain and Charles McLean, NISTIR 7071, December 2003.

[9] Roadmap for Integrated Modeling and Simulation for Emergency Response, Sanjay Jain, Charles McLean et al, June 2004 (draft).

Smart Sensor Networks and Technologies (Objective #4)

The development and use of sensors and sensor networks will be critical for the detection of chemical, biological, radiological, nuclear, and explosive weapons and means for their delivery.[10] Currently these systems are being conceived, developed, and deployed on a local/regional basis. Until a common overall standards-based architecture is defined for these systems, it is all but certain that there will be duplication of effort in the engineering and integration required to set them up. Furthermore, if standards are not adopted relatively early in the development and deployment of these systems, they will not be interoperable. This will greatly increase long-term costs and compromise capability and performance. In this new-start project, we will begin to address these issues by identifying user needs and surveying the standards landscape related to smart sensor networks for homeland security. We will identify existing standards that can be applied in the short term, as well as gaps in standards coverage that will need to be addressed in the future. We will also identify where test methods need to be developed for standards validation and conformance. This project will leverage through collaboration existing efforts in this area, including the Oak Ridge National Laboratory's SensorNet program, the Open Geospatial Consortium's Critical Infrastructure Protection Initiative, and Institute of Electrical and Electronics Engineers (IEEE) 1451 (Standard for a Smart Transducer Interface for Sensors and Actuators) working group projects.

Standard Reference Materials for Bullets and Casings (Objective #5)

The National Integrated Ballistics Information Network (NIBIN) is currently under development by Bureau of Alcohol, Tobacco, and Firearms (ATF) and the Federal Bureau of Investigation (FBI). One of the key steps is to establish measurement unification and information sharing in ballistics measurements using the IBIS (Integrated Ballistics Identification System) and other systems. However, to demonstrate completely the reliability and measurement control of these systems, high quality measurement standards for bullets and casings are required. Their key properties include uniformity, reproducibility and measurement traceability. These standard bullets and casings serve as check standards from day to day for each system and will ensure consistency between systems. Now that reference materials for bullets are nearly in place and those for casings will soon follow, the measurement system must be established through laboratory comparisons and refinement of the measurement procedures. In addition, supporting research to improve the cost, chemical stability, and mechanical stability of the standards would be vital to crime labs.

[10] Making the Nation Safer: The Role of Science and Technology in Countering Terrorism

Evaluation of Ballistic Imaging Technology (Objective #6)

The purpose of this project is to evaluate the feasibility of the creation and maintenance of a ballistic database, which would consist of digital images and ballistic signature representations of firearms manufactured and imported for sale in the U.S. The technical approach is designed to examine the two fundamental premises of ballistic signature for such a database: 1) the extent to which ballistic markings are unique to individual firearms; and 2) the extent to which the signature of an individual firearm persists over some expected number of repeat firings and remains differentiable from other individuals. The study aims to test the theory of the toolmark signature uniqueness and persistence in the context of topographic measurement of the markings impressed upon surfaces of bullets and shell casings. For that purpose, it will be helpful to use standard bullets and casings being developed by NIST in a separate project to check the reproducibility of different firearm identification and measurement systems. Once the physical basis of toolmark signatures is verified and their dynamics characterized, the study will assess the suitability and limitations of current databases for firearms.

Ballistic Resistant Body Armor and Bullet Studies (Objective #7)

This work involves developing and conducting tests and analytical methods to characterize dynamic properties of bullet and soft body armor materials. The results of these tests will be used to develop a dynamic material properties database for bullet and armor materials, including high rate and heating effects. Special attention will be directed at frangible and other special materials/designs that pose a potential threat to existing armor. Both PBO (Zylon) and Aramid (Kevlar) fiber based soft body armor will be included in the studies. The benefits of this work will be better protective devices for law enforcement personnel, firefighters and other first responders relying on protective equipment. The designers of protective equipment and ammunition will be the initial users of the results of this project. In the future the designers will rely more on modeling and simulation, similar to other manufacturing processes, and accurate material properties will be essential to this modeling effort. Incorporating accurate properties for the materials in the modeling will reduce the number of prototypes that need to be tested and result in a better design more rapidly developed. This in turn will shorten the time from initial concept to equipment in use by law enforcement officers, and dramatically increase the pace at which improved protective equipment becomes available to first responders.

Emergency Vehicle Sirens (Objective #8)

The project will result in improved measurement methods and more comprehensive tests for certifying siren systems and components that are used on vehicles operated by emergency first responders. These sirens provide audible warning that the vehicles are nearby, responding to an emergency, and calling for the right-of-way. These measurements and tests will be developed by government and industry representatives with expertise in acoustical measurements, electrical measurements and/or environmental testing of aftermarket warning equipment for emergency vehicles. Society of Automotive Engineers (SAE) standard SAE J1849 is currently used by organizations that need to cite documents or measurement procedures specified in these documents for certification of equipment used by emergency first responders. Organizations that use emergency vehicle sirens certified to SAE J1849 will have a much higher degree of assurance that these devices have been subjected to a thorough and comprehensive set of rigorous tests and requirements.

Typical Customers and Collaborators

Homeland Security Robot Performance Metrics and Standards

DHS Science and Technology (S&T) Directorate, DHS Emergency Preparedness and Response Directorate/ Federal Emergency Management Agency (FEMA), NIJ, Technical Support Working Group (TSWG), Department of Defense (DOD), National Institute for Urban Search and Rescue (NIUSR), RoboCupRescue League, American Association of Artificial Intelligence (AAAI), Mitre, University of Pittsburgh, University of South Florida, University of Massachusetts, Carnegie Mellon University, National Aeronautics & Space Administration (NASA) Disaster Assistance and Rescue Team, and NIST Information Technology Lab (ITL) and Electrical and Electronics Engineering Lab (EEEL), and Building and fire Research Lab (BFRL)

Industrial Control System Security

The over 500 members in the PCSRF include ABB, Emerson Process Management, Honeywell, Invensys, Rockwell, Cisco, Microsoft, Sun Microsystems, American Gas Association, BP, Chevron Texaco, Exxon Mobil, Association of Metropolitan Water Agencies, American Chemistry Council, Dow, Dupont, Eastman Kodak, Schering-Plough, Georgia-Pacific, General Motors, I-4, National Defense University, Idaho National Engineering & Environmental Lab, Pacific Northwest National Lab, Sandia National Lab, DHS Information Analysis and Infrastructure Protection Directorate and The Society of Instrumentation, Systems, and Automation (ISA)

Modeling and Simulation for Emergency Response

Sandia National Labs, University of Southern California, Department of Homeland Security (S&T, Transportation Security Administration, FEMA), National Training Systems Association, Lawrence Livermore National Laboratory, Defense Threat Reduction Agency, Purdue University, Association for Enterprise Integration, National Center for Manufacturing Sciences, Battelle Eastern Science & Technology Center, Defense Modeling & Simulation Office, Argonne National Laboratory, Institute for Defense and Homeland Security, Altarum, University of Southern California, U.S. Air Force, Naval Research Laboratory, U.S. Joint Fighting Command, U.S. Army STRICOM (Simulation, Training & Instrumentation Command), U.S. Army Training - TRADOC (Training & Doctrine Command) Analysis Center, Oak Ridge National Laboratory, U.S. Army RDECOM (Research Development and Engineering Command), and Institute for Defense Analysis

Smart Sensor Networks and Technologies

Oak Ridge National Laboratories, IEEE 1451 member companies, NIST ITL and BFRL

Standard Reference Materials for Bullets and Casings

NIJ, and NIST EEEL/Office of Law Enforcement Standards (OLES)

Evaluation of Ballistic Imaging Technology

NIJ, NIST EEEL/OLES, and NIST Materials Science and Engineering Lab (MSEL)

Ballistic Resistant Body Armor & Bullet Studies

NIJ, NIST EEEL/OLES, and MSEL

Emergency Vehicle Sirens

NIJ, and NIST EEEL/OLES

FY2005 Standards Participation

Homeland Security Robot Performance Metrics and Standards

ASTM International, IEEE, NIUSR, Joint Architecture for Unmanned Systems Working Group, and NIJ

Industrial Control System Security

ISA SP-99 Industrial Control Security committee, American Gas Association AGA-12 committee, International Electrotechnical Commission (IEC) 617842, ISO, ASTM E54 committee on Homeland Security Applications, and Open DeviceNet Vendors Association

Modeling and Simulation for Emergency Response

IEEE High Level Architecture

Smart Sensor Networks and Technologies

IEEE Technical Committee on Sensor Technology/P1451 working groups, and Open Geospatial Consortium

Standard Reference Materials for Bullets and Casings

NIJ

Evaluation of Ballistic Imaging Technology

NIJ

Ballistic Resistant Body Armor and Bullet Studies

NIJ

Emergency Vehicle Sirens

NIJ, SAE

Homeland & Industrial Control Security